主向位科技股份有限公司
CTC UNION TECHNOLOGIES CO., LTD.

Product Security Advisory

CVE-2023-48795 – Terrapin SSH Attack

Reference ID: TEL-GSW-26111602 **Issue Date: 2026/11/16**

CVE ID: CVE-2023-48795

CVSSv3: 5.9 (Medium)

Issue Description

A flaw was found in the SSH channel integrity. By manipulating sequence numbers during the handshake, an attacker can remove the initial messages on the secure channel without causing a MAC failure. For example, an attacker could disable the ping extension and thus disable the new countermeasure in OpenSSH 9.5 against keystroke timing attacks. For more information about this vulnerability, see CVE-2023-48795 page.

Affected Products

GSW-3424CM
GSW-4424CM
GSW-3424MP
GSW-4424MP(H)

Mitigations

A newer firmware is released to remove chacha20-poly1305 encryption algorithm.

Model	Old Firmware Version	New Firmware Version	Firmware Request
GSW-3424CM	1.01	1.02	Technical Support
GSW-4424CM	1.01	1.02	Technical Support
GSW-3424MP	1.03	1.04	Technical Support
GSW-4424MP(H)	1.03	1.04	Technical Support